CLAIMS

What is claimed is:

1. A method for an authentication process within a data processing system, the method comprising:

receiving at a single sign-on (SSO) agent an initial authentication request for a user;

authenticating the user at the SSO agent for the initial authentication request;

retrieving by the SSO agent an attribute certificate associated with the user; and

authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

2. The method of claim 1 further comprising:

retrieving a private key associated with the user;

extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

3. The method of claim 1 further comprising:

forwarding the authentication data to a protected resource.

4. The method of claim 3 wherein the protected resource is a legacy application.

5. The method of claim 3 further comprising:

approving the user for access to the protected resource based on the authentication data.

6. The method of claim 3, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the method further comprising:

parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

7. The method of claim 1 wherein the authentication data comprises a user identity and a password.

8. The method of claim 1 wherein the attribute certificate is formatted according to an X.509 standard.

9. A data structure representing an attribute certificate for use in a data processing system, the data structure comprising:

an issuer name;

a signature;

a holder name;

an attribute containing encrypted authentication data that was generated by encrypting multiple sets of authentication data for protected resources with a public key associated with a user by a network single sign-on (SSO) agent.

10. The data structure of claim 9 wherein the protected resource is a legacy application.

11. An apparatus for an authentication process within a data processing system, the apparatus comprising:

means for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

means for authenticating the user at the SSO agent for the initial authentication request;

means for retrieving by the SSO agent an attribute certificate associated with the user; and

means for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

12. The apparatus of claim 11 further comprising:

means for retrieving a private key associated with the user;

means for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

means for decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

13. The apparatus of claim 11 further comprising:

means for forwarding the authentication data to a protected resource.

14. The apparatus of claim 13 wherein the protected resource is a legacy application.

15. The apparatus of claim 13 further comprising:

means for approving the user for access to the protected resource based on the authentication data.

16. The apparatus of claim 13, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the apparatus further comprising:

means for parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

17. The apparatus of claim 11 wherein the authentication data comprises a user identity and a password.

18. The apparatus of claim 11 wherein the attribute certificate is formatted according to an X.509 standard.

19. A computer program product in a computer-readable medium for use in a data processing system for an authentication process, the computer program product comprising:

instructions for receiving at a single sign-on (SSO) agent an initial authentication request for a user;

instructions for authenticating the user at the SSO agent for the initial authentication request;

instructions for retrieving by the SSO agent an attribute certificate associated with the user; and

instructions for authenticating the user for subsequent authentication requests via the SSO agent using authentication data within the attribute certificate.

20. The computer program product of claim 19 further comprising:

instructions for retrieving a private key associated with the user;

instructions for extracting encrypted authentication data from the attribute certificate, wherein the encrypted authentication data was generated by encrypting authentication data with a public key associated with the user; and

instructions for decrypting the encrypted authentication data locally using the private key associated with the user in order to extract authentication data for a protected resource.

21. The computer program product of claim 19 further comprising:

instructions for forwarding the authentication data to a protected resource.

22. The computer program product of claim 21 wherein the protected resource is a legacy application.

23. The computer program product of claim 21 further comprising:

instructions for approving the user for access to the protected resource based on the authentication data.

24. The computer program product of claim 21, wherein the attribute certificate contains multiple sets of authentication data for multiple protected resources, the computer program product further comprising:

instructions for parsing the authentication data to retrieve a specific set of authentication data for the protected resource.

25. The computer program product of claim 19 wherein the authentication data comprises a user identity and a password.

26. The computer program product of claim 19 wherein the attribute certificate is formatted according to an X.509 standard.